STATE OF ALABAMA

Information Technology Baseline

Baseline 660-02B2: Client Security – Windows XP

1. INTRODUCTION:

Hardening IT systems results in a substantial reduction in vulnerability exposure and improves the effectiveness of the enterprise security program. These security settings provide the hardening requirements needed to establish a security baseline for Windows XP client systems in a managed enterprise environment.

2. OBJECTIVE:

Establish a secure baseline configuration for client devices (workstations, laptops, etc.) that utilize Windows XP Professional.

3. SCOPE:

Enterprise client systems running Windows XP Professional with Service Pack 2.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-68: Guidance for Securing Microsoft Windows XP Systems, State of Alabama organizations shall configure enterprise (managed) Windows XP systems in accordance with the following settings:

Note: Effective implementation of these settings requires extensive planning and testing. Personnel with limited Windows XP administration and security experience are cautioned not to apply these security settings to systems on their own.

Note 2: Refer to the NIST source document for security settings for legacy, stand-alone, and specialized security-limited functionality (SSLF) systems. Download this document at: http://csrc.nist.gov/itsec/download_WinXP.html.

4.1 PASSWORD POLICY SETTINGS

Password policy settings are defined in State IT Standard 620-03S1: Authentication-Passwords.

4.2 ACCOUNT LOCKOUT POLICY SETTINGS

The following Account Lockout Policy settings shall be defined in the Default Domain Policy and applied at the domain level in an Active Directory.

Table 4-2: Account Lockout Policy Settings

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

4.3 AUDIT POLICY SETTINGS

Table 4-3: Audit Policy Settings

Policy	Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Not defined (not applicable)
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing (see note)
Audit system events	Success

Note: Enabling this setting will generate many events; use only when absolutely necessary.

4.4 USER RIGHTS ASSIGNMENT SETTINGS

Applying the principle of least privilege, each group has only the necessary rights, and users belong only to the necessary groups. Apply the following user rights assignment settings:

Table 4-4: User Rights Assignment Settings

Policy	Setting
Access this computer from the network	Not defined
Act as part of the operating system	None
Add workstations to domain	Administrators
Adjust memory quotas for a process	Not defined
Allow log on locally	Users, Administrators
Allow logon through terminal services	Not defined
Back up files and directories	Not defined
Bypass traverse checking	Not defined
Change the system time	Administrators
Create a pagefile	Administrators
Create token object	Not defined
Create global objects	Not defined
Create permanent shared objects	Not defined
Debug programs	Administrators
Deny access to this computer from the network	Guest, SUPPORT_388945a0
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Deny logon through Terminal Services	Not defined

Policy	Setting
Enable computer and user accounts to be trusted for delegation	Not defined
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE, NETWORK SERVICE
Impersonate a client after authentication	Not defined
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	None
Log on as a batch job	Not defined
Log on as a service	Not defined
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Not defined
Profile system performance	Administrators
Remove computer from docking station	Users, Administrators
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Not defined
Shut down the system	Users, Administrators
Synchronize directory service data	Not defined (not applicable)
Take ownership of files or other objects	Administrators

4.5 SECURITY OPTIONS SETTINGS

To achieve greater security than the default settings provide, Security Options shall be modified as follows:

Table 4-5: Security Options Settings

Policy	Setting
Accounts: Administrator account status	Not defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Not defined (Rename the built-in account with a nonstandard value)
Accounts: Rename guest account	Not defined (Rename the built-in account with a nonstandard value)
Audit: Audit the access of global system objects	Not defined
Audit: Audit the use of Backup and Restore privilege	Not defined
Audit: Shut down system immediately if unable to log security audits	Not defined (Reflect the local organizational policy)
DCOM: Machine Access Restrictions in Security Descriptor Definition Language SDDL) syntax	Not defined (If enabled, this may prevent the use of Remote Assistance)
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not defined (If enabled, this may prevent the use of Remote Assistance)
Devices: Allow undock without having to log on	Not defined

Policy	Setting
Devices: Allowed to format and eject removable media	Administrators and Interactive Users
Devices: Prevent users from installing printer drivers	Enabled; Disabled for laptops
Devices: Restrict CD-ROM access to locally logged-on user only	Not defined
Devices: Restrict floppy access to locally logged-on user only	Not defined
Devices: Unsigned driver installation behavior	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not defined
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	Replace with a local organization approved logon banner
Interactive logon: Message title for users attempting to log on	Replace with a local organization approved logon banner
Interactive logon: Number of previous logons to cache (in case domain controller is not available	2 logons (for highest security, except for laptops, set to 0 logons)
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled; Disabled for laptops and standalones
Interactive logon: Require smart card	Not defined
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled (this will prevent communication with servers prior to Windows 2000)
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled (this will prevent communication with servers prior to Windows NT)
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled

Policy	Setting
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	Not defined
Network access: Remotely accessible registry paths	Not defined
Network access: Restrict anonymous access to named pipes and shares	Not defined
Network access: Shares that can be accessed anonymously	Not defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled (enforce at the domain level)
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM (this will prevent communication with some clients and servers)
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients This will prevent communication with some clients and servers.	Require message integrity Require message confidentiality Require NTLMv2 session security Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers This will prevent communication with some clients and servers.	Require message integrity Require message confidentiality Require NTLMv2 session security Require 128-bit encryption
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Not defined
Shutdown: Allow system to be shut down without having to log on	Not defined
Shutdown: Clear virtual memory pagefile	Enabled (this can cause reboots to take longer, especially on systems with large amounts of RAM)
System cryptography: Force strong key protection for user keys stored on the computer	Not defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled (configure TLS support in Internet Explorer, otherwise IE might be prevented from connecting to certain Web sites)
System objects: Default owner for objects created by members of the Administrators group	Object creator
System objects: Require case insensitivity for non-Windows subsystems	Not defined
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	Not defined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not defined

4.6 EVENT LOG POLICIES

Windows XP records information about significant events in three logs: the Application Log, the Security Log, and the System Log. Enable logging for all three types of logs, protect access to the logs, and specify the maximum log size.

Table 4-6: Event Log Policies

Policy	Setting
Maximum application log size	16384 kilobytes
Maximum security log size	81920 kilobytes
Maximum system log size	16384 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed

These log sizes are the smallest required maximums and should be increased if additional space is available. If the maximum log size is set too low, the system may not have enough room for storing information on system activity.

Additional logging requirements for all systems are defined in State IT Standard 670-06S1: Log Management.

4.7 RESTRICTED GROUPS

Remove all users from the Remote Desktop Users and Power Users groups. If local policy requires the usage of these groups, be certain to add only the users requiring membership.

4.8 SYSTEM SERVICES

All unnecessary services shall be disabled to reduce the number of attack vectors against the system. In managed environments, the Group Policy Object should be used to configure services on systems; in other environments, services can be shut off individually on each system.

The following services shall be disabled in all environments unless there is a specific and documented need that requires them to be enabled:

Alerter (Windows XP SP 2 disables the Alerter service by default)
ClipBook
FTP Publishing Service
IIS Admin Service
Messenger (Windows XP SP 2 disables the Messenger service by default)
NetMeeting Remote Desktop Sharing

Routing and Remote Access
Simple Mail Transfer Protocol (SMTP)
Simple Network Management Protocol (SNMP) Service
Simple Network Management Protocol (SNMP) Trap
Simple Service Discovery Protocol (SSDP) Discovery Service
Telnet
World Wide Web Publishing Services

For additional security, disable these other services:

Computer Browser
Fax
Indexing Service
Remote Desktop Help Session Manager
Task Scheduler
Terminal Services
Universal Plug and Play Device Host

4.9 FILE PERMISSION SETTINGS

Permission settings for the following files (located in %SystemRoot%\system32\) shall be set to Administrators: Full and System: Full.

arp.exe	net1.exe	rexec.exe
at.exe	netsh.exe	route.exe
attrib.exe	netstat.exe	rsh.exe
cacls.exe	nslookup.exe	sc.exe
debug.exe	ntbackup.exe	secedit.exe
edlin.exe	rcp.exe	subst.exe
eventcreate.exe	reg.exe	systeminfo.exe
eventtriggers.exe	regedit.exe	telnet.exe
ftp.exe	regedt32.exe	tftp.exe
nbtstat.exe	regini.exe	tlntsvr.exe
net.exe	regsvr32.exe	

4.10 REGISTRY PERMISSIONS

Set restrictive permissions for several registry keys and values to protect them from unauthorized access and modifications. Changing registry permissions can negatively impact the functionality and stability of Windows XP systems, so administrators should carefully test any such permissions before deploying them on production systems.

The following tables provide the registry key name and path, describe its purpose, and recommend an appropriate setting.

Note: HKLM is an abbreviation for HKEY_LOCAL_MACHINE.

Table 4-7: Registry Settings

Item Registry Value Name and Path Recommended	Data Value	Explanation
HKLM\System\CurrentControlSet\Services\ IPSec\NoDefaultExempt	1	In Windows XP, IPsec has certain default exemptions to its policy filters. This parameter should usually be set to 1, which removes the exemptions for Kerberos and RSVP traffic.
HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer\NoDriveTypeAutoRun	255	The autorun feature attempts to run content from a CD automatically when it is placed in the system. If a CD contains malicious content, it could be automatically run. Setting this registry value to 255 disables the autorun feature for all types of drives.
HKLM\System\CurrentControlSet\Control\ SessionManager\SafeDllSearchMode	1	Windows XP searches directories in a particular order when it is looking for a file to execute. By default, Windows searches the current directory before the Windows and system directories. Setting this parameter to 1 causes Windows to search the Windows and system directories before searching the current directory. This is a better security practice because the current directory may be less restrictive than the Windows and system directories.
HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\ScreenSaverGracePeriod	0	This value sets the grace period between the activation of a password-protected screen saver and the requirement to enter a password to unlock the system. Setting this value to 0 eliminates the grace period.
HKLM\System\CurrentControlSet\Services\ CDrom\Autorun	0	Setting this value to 0 disables the autorun feature for CDs.
HKLM\Software\Microsoft\DrWatson\ CreateCrashDump	0	Memory dumps can contain sensitive information such as passwords. Setting this value to 0 disables the creation of a memory dump file by the Dr. Watson program debugger. This setting should be enabled to troubleshoot a recurring problem.
HKLM\Software\Microsoft\WindowsNT\ CurrentVersion\AEDebug\Auto	0	Setting this value to 0 disables Dr. Watson.
HKLM\System\CurrentControlSet\Services\ Tcpip\Parameters\PerformRouterDiscovery	0	This parameter controls whether the system attempts to perform router discovery per RFC 1256 on a per-interface basis. This feature should be disabled by setting the value to 0.
HKLM\System\CurrentControlSet\Services\ Tcpip\Parameters\TcpMaxHalfOpen	100	This setting specifies the number of connections permitted in the SYN-RCVD state before SynAttackProtect measures are implemented.
HKLM\System\CurrentControlSet\Services\ Tcpip\Parameters\TcpMaxHalfOpenRetried	80	This setting specifies the number of connections permitted in the SYN-RCVD state for which at least one retransmission of the SYN has been sent, before SynAttackProtect measures are implemented.

Item Registry Value Name and Path Recommended	Data Value	Explanation
HKLM\System\CurrentControlSet\Services\ Tcpip\Parameters\TCPMaxPortsExhausted	5	This setting specifies how many connection requests can be refused before SynAttackProtect measures are implemented.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 620-03S1: Authentication-Passwords

Information Technology Standard 670-06S1: Log Management

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/14/2008	